U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RIC 2011

Learning From Digital System Experience

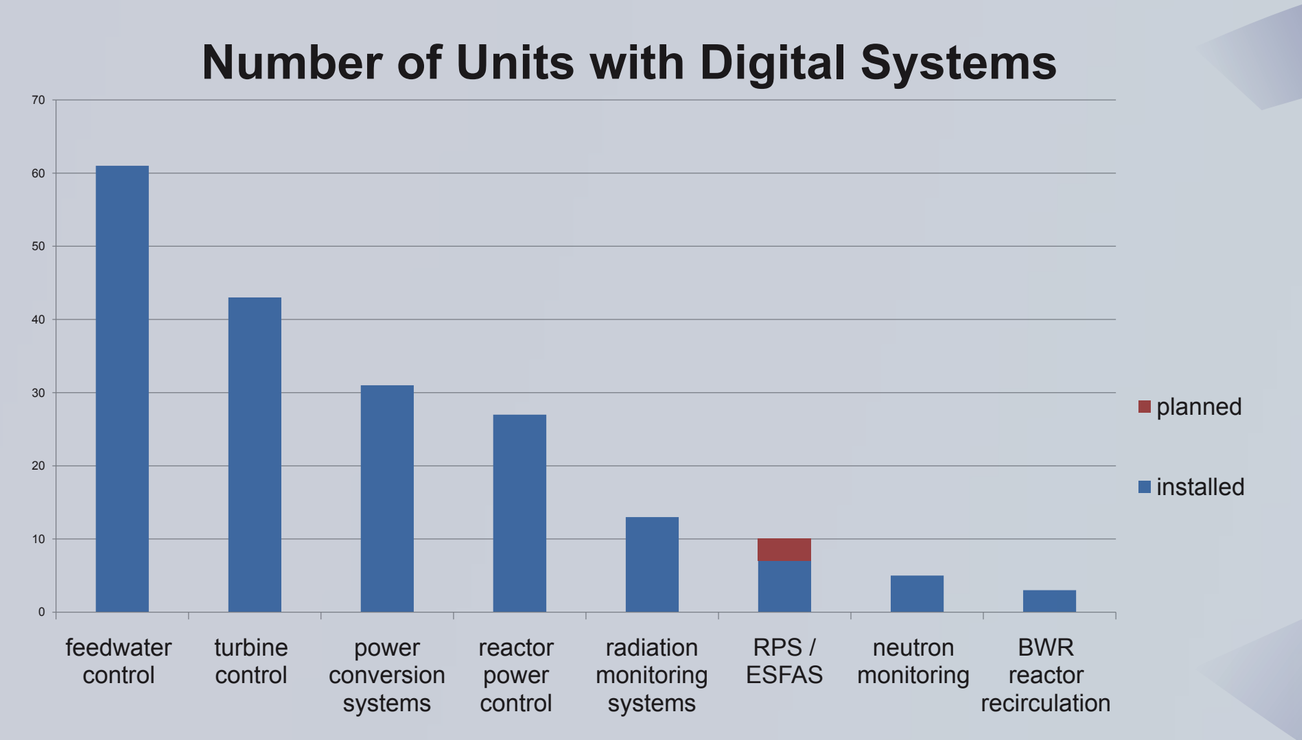
"Every event is a learning opportunity"–*Sushil Birla*

Improved Regulatory Guidance

Domestic

Inventory and Classification

Identify digital systems used in nuclear power plants and apply a classification structure (function, components, life cycle).



Number of Units with Digital Systems
70
60
50
40
30
20
10
0
planned
installed
feedwater control
turbine control
power conversion systems
reactor power control
radiation monitoring systems
RPS / ESFAS
neutron monitoring
BWR reactor recirculation

Learning Experience

Mining existing data sources such as licensee event reports and Equipment Performance and Information Exchange System (EPIX) is difficult.

Software and interconnection information is not available from existing data sources.

Direct contact with the plants is needed to obtain information on system configuration, software, and interconnections.

NRC and industry should work together to enhance digital inventory data structure and information.

Next Steps

Work with the Institute of Nuclear Power Operations (INPO) and industry to develop enhanced methods for collecting and extracting digital information.

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

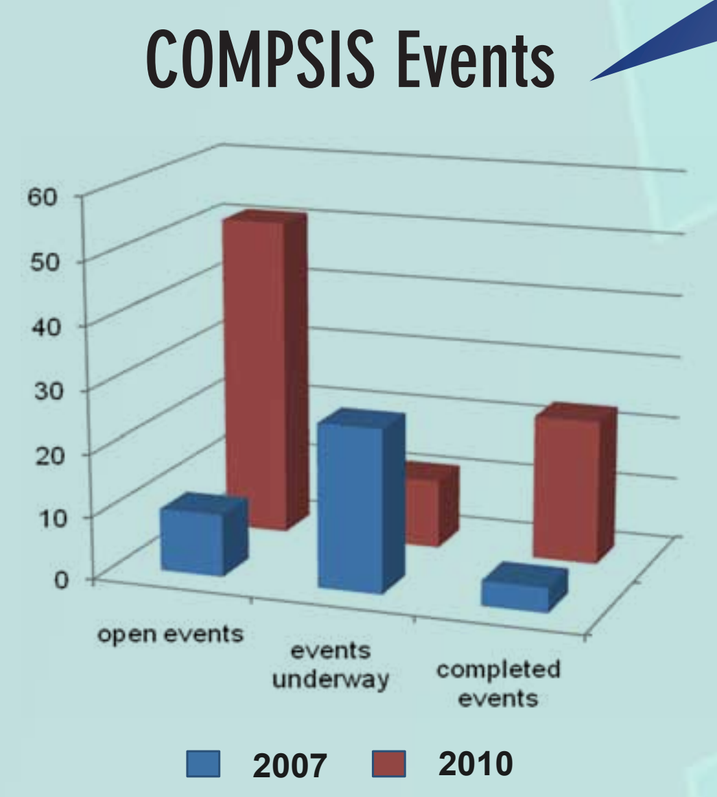
Improve digital instrumentation and control methods, tools, data, and technical information useful to the U.S. nuclear industry and the U.S. Nuclear Regulatory Commission (NRC).

International

Learning Experience

Well-defined requirements can improve system safety and reliability.

Main root causes are design defects, problems with configuration management, and hardware failures.



Lungmen Advanced Control Room

COMPSIS

COMPuter-based Systems Important to Safety

International participation in collecting information on fault experiences with computer-based safety systems at nuclear power plants.

Next Steps

- Continue adding research-grade events.
- Add new lower-severity events to the database.
- Compare data structure with other databases, e.g., Working Group on Risk Assessment (WGRisk).

Other Collaborative Activities

INER · IRSN Institut de Radioprotection et de Sûreté Nucléaire · STUK · The OECD Halden Reactor Project · EDF · KAERI Korea Atomic Energy Research Institute

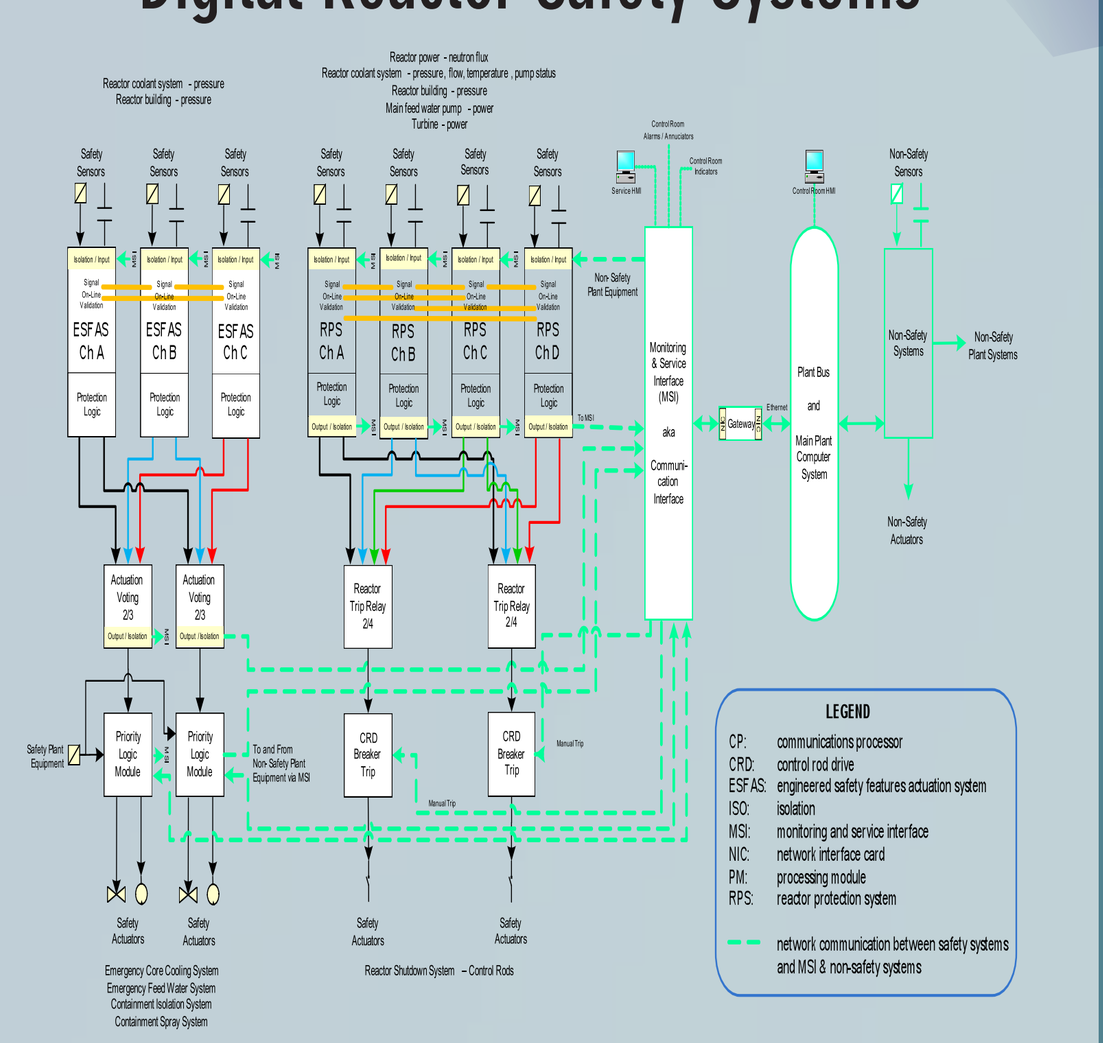
Methods and Tools

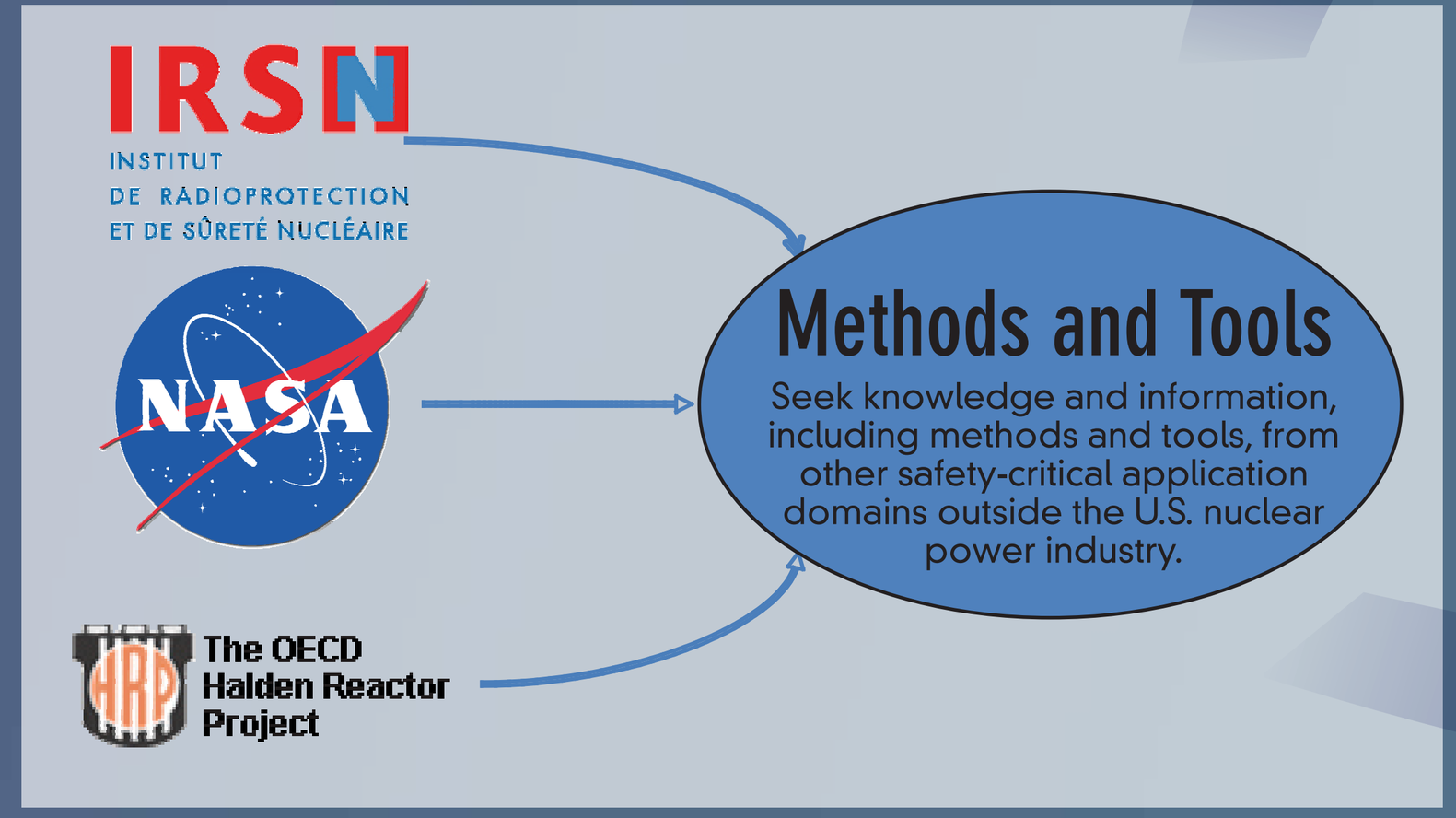
Learning Experience

Lack of adequate understanding of how digital instrumentation and control systems fail.

No universally accepted way to categorize failure data.

Digital Reactor Safety Systems



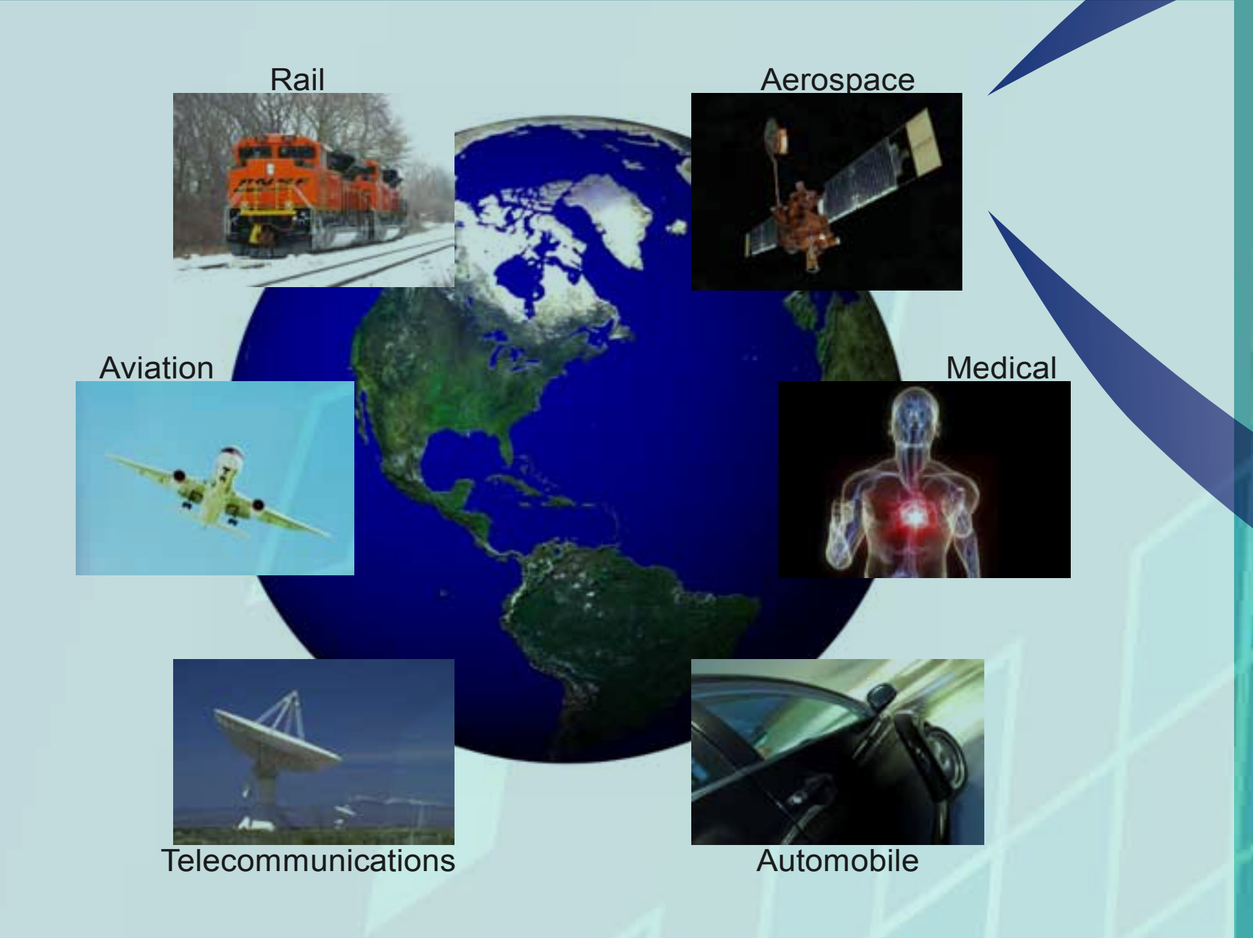


IRSN
INSTITUT DE RADIOPROTECTION ET DE SÛRETÉ NUCLÉAIRE
NASA
The OECD Halden Reactor Project
Methods and Tools
Seek knowledge and information, including methods and tools, from other safety-critical application domains outside the U.S. nuclear power industry.

Next Steps

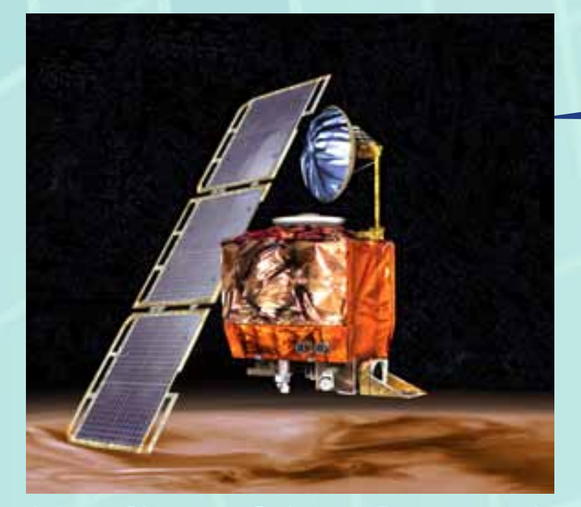
- Support a consistent structure for categorizing failure data.
- Research methods for data mining and learning.
- Develop a framework for organizing information.

Non-Nuclear



Learning Experience

- More careful and consistent documentation of minor incidents correlates with fewer major incidents.
- While incident frequency drops over time, it will increase whenever new conditions are encountered.



Mars Climate Orbiter: Destroyed because of a mismatch in units between reused software and new software.
Courtesy of http://www.jpl.nasa.gov/pictures/solar/mcoartist.html

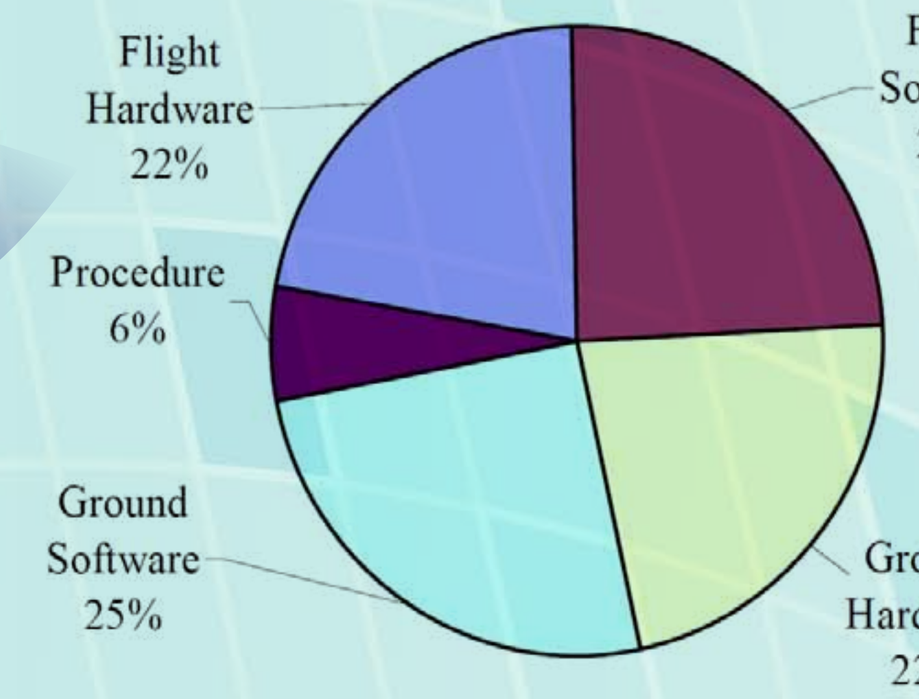
Next Steps

Opportunity: Still collecting information on Mars as well as operating experience in digital error detection and correction.
Courtesy of NASA/nasaimages.org

- Gain insight into diagnostics and prognostics.
- Investigate whether the root causes of minor and major events differ.
- Evaluate emerging technologies.
- Investigate NASA software rigor at different quality categories and compare to NPP software rigor.

NASA/Jet Propulsion Laboratory Data

The Jet Propulsion Laboratory database includes thousands of systematically documented digital instrumentation and control events that occurred during National Aeronautics and Space Administration (NASA) missions.



Anomaly source percentages for all NASA missions to Mars from launch to arrival, 1990 to 2004.

Source: N. Green, A. Hoffman, T. Schow, and H. Garrett, "Anomaly Trends for Robotic Missions to Mars: Implications for Mission Reliability," 44th American Institute of Aeronautics and Astronautics Aerospace Sciences Meeting and Exhibit, Reno, Nevada, January 9–12, 2006.